|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | KITRI 모의해킹 28기 | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | 작성:염찬호 | | |  | |
|  | Sniffing | | | | | | |  |
|  | | -Switch Jamming- | | | |  | | |
|  | |  | | | |  | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |
|  | | |  | |  | | | |

|  |
| --- |
| 1. 개요(공격개념/원리/취약점/공격 시 예상피해 등) |
|  |
| 1. Switch jamming attack 이란? |
| * 위조된 매체 접근제어(MAC) 주소를 지속적으로 네트워크로 흘려 보내 스위치 저장 기능을 혼란 시켜 더미 허브 (dummy hub)처럼 작동하도록 하는 공격이다. 스위치를 직접 공격하며, MAC테이블을 위한 캐시 공간에 버퍼 오버플로 공격을 실시하는 것과 같다. |
| 1. 원리 |
| * 스위치에 랜덤한 형태로 생성한 MAC Address를 가진 패킷을 무한대로 보내면, 스위치에 해당 MAC address가 등록이 되어 MAC Table은 자연스럽게 저장용량을 넘게 되어 스위치의 원래 기능을 읽고 더미 허브처럼 작동하게 된다. 즉, 스위치는 Fowarding이 아닌 Broadcast하게 만드는 것이다. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 2. 공격과정 (필요시 가정이나 예상 시나리오 포함) |
| 실습 환경  공격자 PC(kali linux)1.1.1.12/25  공격 대상 PC1(Cent Os)1.1.1.10/25  공격 대상 PC2(Cent OS)1.1.1.11/25 |
| 1. 공격 수행 |
| * 공격 전 Switch의 Mac address테이블을 확인한다. * #show mac-address-table |
| * #show mac-address-table count      * 공격자 PC에서 아래와 같은 명령어 입력으로 연결되어 잇는 스위치에 임의의 mac주소를 보낸다. * #macof (해당 툴이 없을 경우 apt-get install dsniff를 설치 해준다.)      * 다량의 mac주소가 스위치에 전송되는 것을 확인 할 수 있다. |
| 1. 공격자 PC 패킷 분석 |
| * 스위치에게 다량의 ARP 메시지를 보내는 것을 확인할 수 있다. |

|  |
| --- |
|  |
| 3. 공격 결과 |
|  |
| 1. 비정상적인 mac주소 |
| * 스위치에서 다시 MAC 주소를 확인해보면 MAC주소의 개수가 8189개까지 증가한 것을 확인할 수 있다. * #show mac-address-table count |
| 1. 다른 서버간 통신 패킷 확인 |
| * Switch의 Mac Table이 꽉 차게 되어 Switch는 Hub처럼 동작하게 되어서 타 서버 간의 통신 패킷을 확인할 수 있게 된다. |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
|  |
| 4. 보안진단 및 대책 |
|  |
| 1. Port Security 설정 1 |
| * 전제 조건 * Dynamic Port 설정 불가(Trunk, Access포트만 설정 가능) * Span의 목적지 포트에는 적용 불가 * Ether Channel에 설정 불가 * 포트에 학습할 수 있는 Mac주소의 수를 제한하는 방법이다. * #interface fa0/0 * #switchport port-security maximum 2 * #swiotchport port-security mac-address xxxx.xxxx.xxxx |
|  |
| 1. Port Security 설정 2 |
| * 정책 위반 시 대응 방법을 설정하는 방법 * #interface fa0/0 * #swithport port-security violation {shutdown | protect | restrict} * Shutdown : 예를 들어 위와 같이 2개 이상을 넘어가면 shutdown 같은 경우 서버를 꺼버린다. * Protect : 위반된 트래픽을 drop 시킨다. * Restrict: 위반되었다는 log를 발생시켜 관리자가 확인할 수 있도록 한다. |

|  |
| --- |
|  |
| 5. 보안대책 적용시 공격결과 (최종 매뉴얼에 포함) |
|  |
| 1. Port Security 설정 1이 되었을 경우(현재 스위치에서 사용 불가 L3스위치 가능) |
| * Switch에서 mac-address table을 확인하면 3개가 확인된다. * #show mac-address-table |
| * Switch에 포트로 들어오는 Maximum mac address를 3개로 한정시키고 0000.0000.0001을 수동적으로 입력시켜준다. * #show int fa0/1 * #switchport mode access * #switchport port-security maximum 3 * #switchport port-security mac-address 0000.0000.0001      * 아래와 같이 설정된다. * #show port-security * Maxsecureaddress = 최대 저장 가능한 개수 * Currentaddress = 현재 학습된 개수 * SecurityViolation = 문제된 횟수 * Security Action = Violation의 상태 |
| 1. Port Security 설정 2이 되었을 경우(현재 스위치에서 사용 불가 L3스위치 가능) |
| * Violation 옵션을 사용 * #switchport port-security violation restrict * 스위치는 꺼지지 않으나 통신은 되지 않는다. 즉 restrict로그를 발생한다. |

